

ABSTRACT OF THE DISCLOSURE

A cryptographic communication system in which packet data between terminals is encrypted, and which can reduce the wait time in a decryption apparatus. Packet data transmitted between terminals is encrypted by a transmitting-side cryptographic apparatus and is decrypted by a receiving-side decryption apparatus. The cryptographic apparatus has a fragmentation determination section for deciding whether the packet data should be fragmented, a fragmentation section for dividing the packet data into a plurality of divided data groups if there is a need for fragmentation, the fragmentation section setting the divided data groups in a plurality of divided data packets of a predetermined data structure capable of being reconstructed in a transmission destination terminal, the fragmentation section adding, to each divided data packet, control information for ensuring continuity between the divided data groups, and an encryption section for separately encrypting each of the plurality of divided data packets.